IFW 2132

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants:

Paul C. Kocher, Joshua M. Jaffe, and Benjamin C. Jun

Application No.: 09/930,836

Filing Date: August 15, 2001

Title: Cryptographic Computation Using Masking to Prevent Differential Power Analysis and Other Attacks

Confirmation No.: 2389

Group Art Unit: 2132

Examiner: Herring, Virgil A.

Attorney Docket No.: 44424162-8724

INFORMATION DISCLOSURE STATEMENT

SONNENSCHEIN NATH & ROSENTHAL LLP
Customer No. 26263

Commissioner for Patents
P.O. Box 1450
Arlington, VA 22313-1450

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as First Class Mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date below.

April 26, 2007
date of signature

Edward J. Radlo, Reg. No. 26,793

Sir:

Pursuant to the provisions of 37 CFR § 1.56 and §1.97-§1.98, Applicants hereby submit patents, publications or other information enclosed herewith and listed on the enclosed Form PTO/SB/08a of which they are aware, which they believe may be material to the examination of this application and in respect of which there may be a duty to disclose. This IDS is being filed one month after the filing of a Request for Continued Examination under §1.114 that was filed on March 26, 2007.

A list of the patents and publications is set forth on the enclosed Form PTO/SB/08a. A copy of each of the items on the PTO/SB/08a is supplied herewith, except for the United States Patent documents.

Four of the references are in the Japanese language. English language abstracts are provided for each of these references.

While the information and references disclosed in this Information Disclosure Statement may be "material" pursuant to 37 CFR § 1.56, submission of this IDS is not intended to constitute an admission that any patent, publication or other information referred to herein is "prior art" for this invention unless specifically designated as such.

In accordance with 37 CFR § 1.97(g), the filing of this Information Disclosure Statement shall not be construed to mean that a search has been made or that no other material information as defined in 37 CFR § 1.56(a) exists. It is submitted that this Information Disclosure Statement complies with 37 CFR § 1.98 and MPEP § 609, and the Examiner is respectfully requested to consider the listed references.

Applicants believe no fee is due. However, the Commissioner is hereby authorized to charge our Deposit Account No. 19-3140 for any fees required in connection with the filing of this Information Disclosure Statement. This sheet is being submitted in duplicate.

Respectfully submitted,

date of signature: April 26, 2007

Edward J. Radlo
Reg. No. 26,793
Attorney of Record

SONNENSCHEIN NATH & ROSENTHAL LLP
P.O. Box 061080
Wacker Drive Station, Sears Tower
Chicago, Illinois 60606-1080
(415) 882-2402

cc: IP/T docket CH (w.PTO/SB/08a)
J. Yang (DPA-DES-CON1) (w.PTO/SB/08a)

PTO/SB/08a (09-06)
Approved for use through 03/31/2007. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of info unless it contains a valid OMB control number.

Substitute for form 1449A/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(use as many sheets as necessary)

Sheet 1 of 3

Complete if Known	
Application Number	09/930,836
Filing Date	August 15, 2001
First Named Inventor	Paul C. KOCHER
Art Unit	2132
Examiner Name	Herring, Virgil A.
Attorney Docket Number	44424162-8724

U.S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	1A	US-4,225,962 B1	09-30-1980	Meyr et al.	
	1B	US-4,669,117 B1	05-26-1987	Van Eck	
	1C	US-4,932,057 B1	06-05-1990	Kolbert	
	1D	US-4,937,866 B1	06-26-1990	Crowther et al.	
	1E	US-5,068,894 B1	11/26/1991	Hoppe	
	1F	US-5,086,467 B1	02-04-1992	Malek	
	1G	US-5,157,725 B1	10-20-1992	Lindholm	
	1H	US-5,165,098 B1	11-17-1992	Hoivik	
	1I	US-5,181,243 B1	01-19-1993	Saltwick et al.	
	1J	US-5,216,713 B1	06-01-1993	Lindholm	
	1K	US-5,249,294 B1	09-28-1993	Griffin, III et al.	
	1L	US-5,477,039 B1	12-19-1995	Lisimaque et al.	
	1M	US-5,944,917 B1	11-30-1999	Wuidart	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Number Country Code[3] Number[4] Kind Code[5] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T[6]
	1N	EP 0 452 031 A2	10-16-1991	Ferranti International		☐
	1O	EP 0 563 912 A1	10-06-1993	Data Protection S.R.L.		☐
	1P	JP 10-197610	07-31-1998	Sony Corp		☐
	1Q	JP 10-084223	03-31-1998	Mitsubishi Electric Corp.		☐
	1R	JP 62-260406	11-12-1987	Nippon Electric Co.		☐
	1S	JP 62-082702	04-16-1987	Hewlett-Packard Yokogawa		☐
						☐

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unqiue citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

PTO/SB/08a (09-06)
Approved for use through 03/31/2007. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of info unless it contains a valid OMB control number.

Substitute for form 1449B/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(use as many sheets as necessary)

Sheet 2 of 3

Complete if Known	
Application Number	09/930,836
Filing Date	August 15, 2001
First Named Inventor	Paul C. KOCHER
Group Art Unit	2132
Examiner Name	Herring, Virgil A.
Attorney Docket No.	44424162-8724

OTHER ITEMS – NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
	1T	ANDERSON, Ross et al., "Tamper Resistance - a Cautionary Note", The Second USENIX Workshop on Electronic Commerce Proceedings, Nov. 18-21, 1996, Oakland, CA.	
	1U	CHAUM and Price (Eds.), "IC Cards in High-Security Applications", Advances in Cryptology - Eurocrypt '87, LNCS 304, Amsterdam, NE (1988), pp. 177-199.	
	1V	GOUTAY, J., "Smart Card Applications in Security and Data Protection", Advances in Cryptology - Eurocrypt '84; LNCS 209, Springer-Verlag, Berlin, Germany; (1985) pp. 459-463.	
	1W	GUILLOU, L.C. et al., "Smart Card, a Highly Reliable and Portable Security Device", Advances in Cryptology - CRYPTO '86; LNCS 263, Springer-Verlag, Berlin, Germany; (1987) pp. 464-479.	
	1X	GUILLOU, L.C., "Smart Cards and Conditional Access", Advances in Cryptology - Eurocrypt '84; LNCS 209, Springer-Verlag, Berlin, Germany; (1985) pp. 480-489.	
	1Y	GUTHERY, Scott, "Smart Cards", www.usenix.org/publications/login/1989-5/guthery.html; May, 1989.	
	1Z	HIGHLAND, Harold Joseph, "The Tempest over Leaking Computers", Abacus, Vol. 5(2), Winter 1988, pp. 10-18, 53. http://cryptome.org/tempest-leak.htm	
	2A	ISO/IEC 7816 International Standard, Geneva, CH: Part 1 Physical Characteristics (Ref. No. ISO/IEC 7816-1:1998(E)), Part 1 Amendment Physical Characteristics (Ref. No. ISO/IEC 7816-1:1998/AMD.1:2003(E)), Part 2 Dimensions and Location of the Contacts (Ref. No. ISO/IEC 7816-2:1999(E)).	

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unqiue citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

PTO/SB/08a (09-06)
Approved for use through 03/31/2007. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of info unless it contains a valid OMB control number.

Substitute for form 1449B/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(use as many sheets as necessary)

Sheet 3 of 3

Complete if Known	
Application Number	09/930,836
Filing Date	August 15, 2001
First Named Inventor	Paul C. KOCHER
Group Art Unit	2132
Examiner Name	Herring, Virgil A.
Attorney Docket No.	44424162-8724

OTHER ITEMS – NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
	2B	KRIVACHY, T., "The Chipcard - An Identification Card with Cryptographic Protection", Advances in Cryptology - Eurocrypt '85; LNCS 219, Springer-Verlag, Berlin, Germany (1986) pp. 200-207.	
	2C	KUHN, Markus G. et al., "Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations", Second Workshop on Information Hiding, Portland, Oregon, April 15-17, 1998.	
	2D	MENZES, A.J. et al., Handbook of Applied Cryptography, Chapters 1, 5 and 7; CRC Press, Boca Raton; Florida (1997).	
	2E	MEYER, Carl H. et al., Cryptography -- A New Dimension in Computer Data Security; Ch. 1; John Wiley & Sons, 1982.	
	2F	RANKL et al., Smart Card Handbook, John Wiley & Sons Ltd., 1997, Chs. 2, 3, 8, 13, and pages 84-89, Chichester, England.	
	2G	SCHMIDT, Dick, "Visions on Development in Information Security", TNO Conference, Delft, Netherlands, October 2-3, 1997.	
	2H	SMULDERS, Peter, "The Threat of Information Theft by Reception of Electromagnetic Radiation from RS-232 Cables", Computers and Security, Vol. 9, pp. 53-58, 1990; Elsevier Science Publishers Ltd.	
	2I	WAKERLY, John F., "Introduction to Computers and Programming", Microcomputer Architecture and Programming: The 68000 Family, John Wiley & Sons, New York, N.Y. (1989), Chapter 1, pp 1-16.	

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unqiue citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.